METHOD FOR REPLACING THE CONTENT OF A DATA STORAGE UNIT

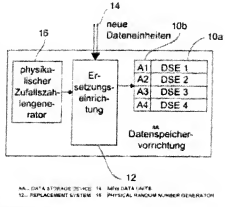
Publication number: DE10216611 (A1)
Publication date: 2003-11-06
Inventor(s): GAMMEL BERNDT [DE]
Applicant(s): INFINEON TECHNOLOGIES AG [DE]
Classification:
- International: ***G06F12/12; G06F21/00;*** **G06F12/12; G06F21/00;** (IPC1-7): G06F12/08
- European: G06F12/12B; G06F21/00N3J5D
Application number: DE20021016611 20020415
Priority number(s): DE20021016611 20020415

Also published as:
WO03088051 (A1)
AU2003229652 (A1)
EP1481327 (A1)
EP1481327 (B1)
TW591391 (B)

Cited documents:
DE19926640 (A1)
EP1179782 (A2)

Abstract not available for DE 10216611 (A1)
Abstract of corresponding document: **WO 03088051 (A1)**

The invention relates to a data storage device comprising a plurality of data storage units (10a), a physical random number generator (16) comprising a noise source which is based on a physical noise process for generating a random number. Said device also comprises a replacement device (12) for selecting a data storage unit wherein data is to be stored dependent on the random number. The security in relation to power analysis attacks is increased by selecting data storage units or lines which are to be replaced in the cache on the basis of authentic random numbers without the need to intervene in the running of the program.



(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 102 16 611 A 1**

(51) Int. Cl.[7]: **G 06 F 12/08**

(21) Aktenzeichen: 102 16 611.0
(22) Anmeldetag: 15. 4. 2002
(43) Offenlegungstag: 6. 11. 2003

DE 102 16 611 A 1

(71) Anmelder:
Infineon Technologies AG, 81669 München, DE

(74) Vertreter:
Schoppe, Zimmermann, Stöckeler & Zinkler, 82049 Pullach

(72) Erfinder:
Gammel, Berndt, Dr.rer.nat., 85570 Markt Schwaben, DE

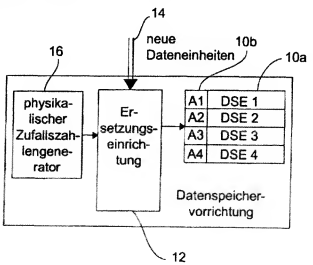
(56) Entgegenhaltungen:
DE 199 26 640 A1
EP 11 79 782 A2
Computer, März 1994, S. 38-46;

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zum Ersetzen eines Inhalts einer Datenspeichereinheit

(57) Eine Datenspeichervorrichtung umfaßt eine Mehrzahl von Datenspeichereinheiten (10a), einen physikalischen Zufallszahlengenerator (16) mit einer Rauschquelle, die auf einem physikalischen Rauschprozeß basiert, zum Erzeugen einer Zufallszahl und eine Ersetzungseinrichtung (12) zum Auswählen einer Datenspeichereinheit, in der Daten zu speichern sind, abhängig von der Zufallszahl. Durch Auswählen von im Cache zu ersetzenden Datenspeichereinheiten bzw. Zeilen auf der Basis von echten Zufallszahlen wird die Sicherheit gegen Leistungsanalyseangriffe erhöht, ohne daß Eingriffe in den Programmablauf nötig sind.



DE 102 16 611 A 1

Beschreibung

[0001] Die vorliegende Erfindung bezieht sich auf Datenspeicherverrichtungen und insbesondere auf einen sicheren Betrieb solcher Datenspeichervorrichtungen.

[0002] Moderne Angriffe auf Datenverarbeitungseinrichtungen die sicherheitsrelevante Daten verarbeiten bzw. auf die darin abgearbeiteten Algorithmen und geheimen Schlüssel erfolgen über sogenannte Leckinformationen. Leckinformationen sind beispielsweise der Stromverbrauch der Datenverarbeitungseinrichtung, eine elektromagnetische Abstrahlung während eines Betriebs der Datenverarbeitungseinrichtung etc. Aus einer statistischen Analyse der aufgenommenen physikalischen Signale kann auf sicherheitsrelevante Informationen rückgeschlossen werden.

[0003] Die bekanntesten Angriffsformen stellen hierbei die einfache Strom- bzw. Leistungsanalyse (Simple Power Analysis = SPA), die differentielle Leistungsanalyse (Differential Power Analysis = DPA) oder Stromanalysen höherer Ordnung (High-Order Differential Power Analysis = HO-DPA) dar.

[0004] Zur Verhinderung dieser Angriffe werden verschiedene Verfahren eingesetzt, wie z. B. softwaretechnische Verfahren durch ständiges Ändern der Abfolge der Operationen des kryptographischen Algorithmus oder durch Einfügen von redundanten Operationen. Hiermit können statistische Auswertungen, beispielsweise des Stromprofiles oder der elektromagnetischen Abstrahlung verhindert oder zumindest erheblich erschwert werden.

[0005] Ein Nachteil dieser Vorgehensweise ist der aufwendige Eingriff in die jeweilige Software und die Algorithmen sowie die in den meisten Fällen resultierende erhebliche Performance-Verringerung. Eine weitere bekannte Abwehrmaßnahme sind zusätzliche Stromprofilgeneratoren, die ein zusätzliches stochastisches Stromprofil dem ursprünglichen Stromprofil der Schaltung, wie z. B. des Controllers etc., überlagern. Der Nutzen dieser Vorgehensweise ist zweifelhaft, da sie im allgemeinen keinen ausreichenden Schutz gegenüber einer DPA oder HO-DPA gibt und außerdem zu einer erheblichen Erhöhung des Stromverbrauchs der Datenverarbeitungseinrichtung führen kann.

[0006] Eine weitere bekannte Maßnahme stellt das Einstreuen von zufälligen Aktionen in der Datenverarbeitungseinheit dar. Hierbei werden zufällige Befehlssequenzen und Zustände in Zustandsmaschinen eingestreut, um eine zeitliche Desynchronisation des Befehlsablaufs eines kryptographischen Prozesses zu erzeugen. Damit können das Auffinden von Triggerpunkten in Stromprofilen und eine Stromprofilanalyse mittels Resynchronisation im zeitlichen Verlauf erschwert werden. Die Steuerung, die als "Leerfunktionsgenerator" bezeichnet wird, dient zur Einschleusung von Zufallssequenzen beispielsweise in die Prozessor-Pipeline einer CPU. Eine solche Steuerung hat typischerweise eine erhebliche Komplexität, da sichergestellt werden muß, daß durch die Sicherheitsmaßnahmen die Integrität der bearbeiteten Daten und die Integrität des Befehlsstroms bewahrt werden. So dürfen beispielsweise nicht Register- oder Speicherinhalte fälschlich überschrieben werden. Natürlich darf auch die Kausalität von Instruktionen nicht verletzt werden, usw.

[0007] Moderne Datenverarbeitungseinrichtungen umfassen eine CPU, einen Speicher, wie z. B. einen festen Speicher und einen flüchtigen Speicher sowie einen Cache-Speicher, der erheblich dazu beiträgt, die Rechengeschwindigkeit einer Datenverarbeitungseinrichtung durch schnelle Speicherzugriffe zu erhöhen. Solche leistungsfähigen und schnellen Speichersysteme enthalten typischerweise mehrstufige Cache-Speicher bzw. Pufferspeicher, die Bereiche

des Hauptspeichers temporär halten. Beispiele sind Instruktions-Cache-Speicher, Daten-Cache-Speicher oder TLBs (TLB = Translation Lookasid Buffer), die auch als Adress-Cache-Speicher bezeichnet werden. Solche Datenspeichervorrichtungen sind in verschiedenen Ausprägungen auf jedem Prozessor vorhanden. Assoziativ aufgebaute Cache-Speicher bzw. Speicher im allgemeinen halten eine Mehrzahl von Zeilen, d. h. Datenspeichereinheiten, in denen jeweils ein Datenblock aus dem Hauptspeicher abgelegt werden kann. Ein solcher Speicher wird auch als n-Wege assoziativer Cache-Speicher bezeichnet, wobei n die Anzahl der Datenspeichereinheiten bezeichnet. Eine dieser n-Datenspeichereinheiten wird ausgewählt, um einen neu in den Speicher zu speichernden Datenblock abzulegen. Hierbei wird der vorherig abgelegte Datenblock verdrängt. Der verdrängte Datenblock muß dann neu vom Hauptspeicher geladen werden, wenn er wieder benötigt wird.

[0008] Gewöhnlich wird zur Auswahl der Zeile, in die eine neue Dateneinheit geschrieben werden soll, ein sogenannter LRU-Algorithmus (LRU = Least Recently Used) benutzt, da mit einer solchen Ersetzungsstrategie typischerweise die beste Cache-Performance erzielt werden kann.

[0009] Eine andere, weniger aufwendige bekannte Ersetzungsstrategie ist die sogenannte Random-Replacement-Strategie, bei der die zu überschreibende Datenspeichereinheit zufällig ausgewählt wird. Bei hoher Cache-Assoziativität und großen Speichern kann mit der Random-Replacement-Strategie annähernd die Performance einer wesentlich aufwendiger zu implementierenden LRU-Strategie erreicht werden.

[0010] Der für die Zufallsersetzungsstrategie (Random-Replacement-Stragie) nötige Zufallszahlengenerator ist ein Pseudozufallszahlengenerator auf der Basis einer Schaltung aus rückgekoppelten linearen Schieberegistern (LFSR; LFSR = Linear Feedback Shift Register). Solche Schaltungen aus rückgekoppelten Schieberegistern werden durch einen sogenannten Keim oder Seed in einen definierten Anfangszustand versetzt, wobei dann, ausgehend von diesem definierten Anfangszustand, eine deterministische Folge von Zufallszahlen erzeugt wird, die jedoch eine annähernd zufällige Verteilung hat. Diese Folge ist jedoch dahingehend deterministisch, daß sie immer, wenn der vorbestimmte Keim in das LFSR eingespeist worden ist, exakt wiederholt wird. Wird ein anderer Kern eingespeist, so ergibt sich eine andere, jedoch ebenfalls vollständig wiederholbare Folge von zufällig erscheinenden Zufallszahlen.

[0011] Im Hinblick auf die oben beschriebenen Attacken auf kryptographische Datenverarbeitungseinrichtungen haben solche Pseudozufallszahlengeneratoren bzw. hat die auf diesen Pseudozufallszahlengeneratoren basierende Zufallsersetzungsstrategie den erheblichen Nachteil, daß der Programmablauf immer deterministisch bleibt. Insbesondere würde sich ein Programm nach jedem Neustart der CPU genau gleich verhalten. Dies stellt einen Angriffspunkt für Leitungsanalyseattacken dar.

[0012] Die Aufgabe der vorliegenden Erfindung besteht darin, ein sicheres Konzept zum Speichern von Daten zu schaffen.

[0013] Diese Aufgabe wird durch eine Datenspeichervorrichtung nach Patentanspruch 1 oder durch ein Verfahren zum Ersetzen eines Inhalts einer Datenspeichereinheit einer Datenspeichervorrichtung nach Patentanspruch 11 gelöst.

[0014] Der vorliegenden Erfindung liegt die Erkenntnis zugrunde, daß die Vorteile der geringen Implementation der Zufalsersetzungsstrategie für eine Datenspeichervorrichtung, die mit sicherheitsrelevanten Daten umgeht, ohne Softwareänderung bzw. aufwendige Leerfunktionsgeneratoren beibehalten werden kann, indem statt oder zusätzlich zu

dem Pseudozufallszahlengenerator ein physikalischer Zufallszahlengenerator, d. h. ein Zufallszahlengenerator mit einer Rauschquelle, die auf einem physikalischen Rauschprozeß basiert, eingesetzt wird.

[0015] Eine Ersetzungsstrategie auf der Basis eines physikalischen Zufallszahlengenerators hat den erheblichen Vorteil, daß tatsächlich eine Randomisierung und nicht eine Pseudo-Randomisierung des Leistungsprofiles einer Datenspeichervorrichtung bzw. einer CPU mit einer erfindungsgemäßen Datenspeichervorrichtung erreicht wird.

[0016] Ein weiterer Vorteil der vorliegenden Erfindung besteht darin, daß keine aufwendigen Software-Eingriffe bzw. kein zusätzlicher Stromverbrauch durch die Zufallsersetzungsstrategie auf der Basis von tatsächlichen physikalischen Zufallszahlen eingeführt wird.

[0017] Ein weiterer Vorteil der vorliegenden Erfindung besteht darin, daß die Option besteht, den physikalischen Zufallszahlengenerator mit einem Pseudozufallszahlengenerator zu kombinieren, der typischerweise schneller Zufallszahlen liefert als ein physikalischer Zufallszahlengenerator. Durch Kombinieren der physikalischen Zufallszahlen und der Pseudozufallszahlen kann bereits eine gute Randomisierung des Stromprofiles erreicht werden, beispielsweise dadurch, daß immer nach einer bestimmten Anzahl von Pseudozufallszahlen eine tatsächliche Zufallszahl eingestreut wird, oder daß nach wie vor die Pseudozufallszahlen verwendet werden, um zu ersetzende Cache-Datenspeichereinheiten auszuwählen, wobei jedoch die für den Pseudozufallszahlengenerator verwendeten rückgekoppelten Schieberegister als Keim bzw. Keime Zufallszahlen erhalten. Somit wird sich bei einem Neustart einer CPU die Ersetzungsfolge nicht immer gleich verhalten, sondern tatsächlich abweichen, obgleich dennoch die schnellen und schaltungstechnisch einfach zu implementierenden Pseudozufallszahlengeneratoren verwendet werden. Die Pseudozufallszahlengeneratoren werden jedoch nunmehr von dem physikalischen Rauschgenerator in wählbaren Abständen in einen neuen Ausgangszustand (Seed-Zustand) versetzt.

[0018] Ein weiterer Vorteil der vorliegenden Erfindung besteht darin, daß der Einsatz eines Zufallszahlengenerators für die Cache-Ersetzung einen wesentlichen Grad an Flexibilität mit sich bringt, dahingehend, daß eine skalierbare Sicherheit geschaffen wird. Für hochsicherheitsrelevante Berechnungen kann auf der Basis von Zufallszahlen eine Cache-Zeilenersetzung durchgeführt werden, während für weniger sicherheitsrelevante Daten, für die jedoch ebenfalls noch ein gewisses Maß an Sicherheit benötigt wird, mittels einer Modussteuerungseinrichtung nach bestimmten Kriterien von der Zufallszahlenersetzung auf eine komplett deterministische Ersetzungsstrategie umgeschaltet wird.

[0019] Bevorzugte Ausführungsbeispiele der vorliegenden Erfindung werden nachfolgend bezugnehmend auf die beiliegenden Zeichnungen detailliert erläutert. Es zeigen:

[0020] Fig. 1 ein Blockschaltbild einer erfindungsgemäßen sicheren Datenspeichervorrichtung; und

[0021] Fig. 2 eine Datenspeichervorrichtung gemäß einem bevorzugten Ausführungsbeispiel der vorliegenden Erfindung.

[0022] Zur Gewährleistung einer sicheren und dennoch effizienten Dekorrelation des Daten- und Befehlsstromes in einem modernen Mikroprozessor wird die in Fig. 1 gezeigte Datenspeichervorrichtung eingesetzt. Dieselbe umfaßt eine Mehrzahl von Datenspeichereinheiten **10a**, denen jeweils Adressen **10b** zugeordnet sind. Die Auswahl der Datenspeichereinrichtung findet über eine Adresse statt, die von einer Ersetzungseinrichtung **12** ausgewählt wird, wenn eine neue Dateneinheit über eine Dateneinheiteinleitung **14** in eine Datenspeichereinheit zu schreiben ist. Die Ersetzungseinrichtung wird von einem physikalischen Zufallszahlengenerator **16** angesteuert, um eine Zufallsersetzungsstrategie auf der Basis einer tatsächlichen physikalischen Zufallszahl und nicht auf einer Pseudozufallszahl durchzuführen.

[0023] Der physikalische Zufallszahlengenerator umfaßt eine Rauschquelle, die auf einem physikalischen Rauschprozeß basiert. Beispielhafte Implementierungen bestehen darin, das thermische Rauschen eines Widerstands entweder direkt auszuwerten oder beispielsweise an einen Steuereingang eines spannungsgesteuerten Oszillators anzulegen, um einen größeren "Zufallshub" zu erreichen. Alternativ kann das Schrotrauschen einer Diode als physikaliseber Rauschprozeß eingesetzt werden. Weitere physikalische Rauschprozesse sind bekannt.

[0024] Es sei darauf hingewiesen, daß in kryptographischen Prozessoren ohnehin Zufallszahlengeneratoren vorhanden sind, die eine Rauschquelle, welche auf einem physikalischen Rauschprozeß basiert, umfassen. So muß eine Datenspeichervorrichtung, die zu einem solchen kryptographischen Prozessorsystem gehört, nicht einmal um einen physikalischen Zufallszahlengenerator erweitert werden, da derselbe ohnehin vorhanden ist. Die einzige Modifikation besteht darin, wenn allein auf den physikalischen Zufallszahlengenerator aufgebaut wird, den physikalischen Zufallszahlengenerator des Kryptoprozessorsystems mit der Ersetzungseinrichtung **12** zu verbinden.

[0025] Fig. 2 zeigt ein bevorzugtes Ausführungsbeispiel einer sicheren Datenspeichervorrichtung gemäß der vorliegenden Erfindung. Neben den Datenspeichereinheiten **10a**, der Ersetzungseinrichtung **12** und dem physikalischen Zufallszahlengenerator **16** ist ferner ein Pseudozufallszahlengenerator **18** vorgesehen, der ebenso wie der physikalische Zufallszahlengenerator **16** mit einer Kombinationseinrichtung **20** verbunden ist. Die Ersetzungseinrichtung **12** wird nunmehr nicht direkt vom physikalischen Zufallszahlengenerator angesteuert, sondern mittels eines Ansteuersignals **22**, das in der Kombinationseinrichtung **20** unter Verwendung des physikalischen Zufallszahlengenerators **16** und des Pseudozufallszahlengenerators **18** erzeugt wird. Mit der Ersetzungseinrichtung **12** ist ferner eine Modussteuerungseinrichtung **22** gekoppelt, auf die später eingegangen wird. Der physikalische Zufallszahlengenerator liefert über eine Leitung **16a** Zufallszahlen zur Kombinationseinrichtung **20**. Über eine Leitung **16b**, die als RN Valid bezeichnet wird, signalisiert der physikalische Zufallszahlengenerator der Kombinationseinrichtung **20**, daß er bereit ist. Die Kombinationseinrichtung **20** kann auf den physikalischen Zufallszahlengenerator **16** über eine Steuerleitung **16c** einwirken.

[0026] Der Pseudozufallszahlengenerator **18** liefert seine Pseudozufallszahlen über eine Leitung **18a** der Kombinationseinrichtung **20**. Der Pseudozufallszahlengenerator **18** ist ferner über eine PRN Valid-Leitung **18b** mit der Kombinationseinrichtung **20** verbunden, die wiederum über eine Steuerleitung **18c** auf den Pseudozufallszahlengenerator **18** einwirken kann. Auf der Leitung **22** liefert die Kombinationseinrichtung **20**, wie es ausgeführt worden ist, der Ersetzungseinrichtung **12** eine Folge von Ansteuersignalen, von denen abhängig die Ersetzungseinrichtung **12** Datenspeichereinheiten auswählt, die durch einen aktuellen zu schreibenden Wert überschrieben werden sollen. Über eine Leitung **24** kann die Ersetzungseinrichtung **12** auf die Kombinationseinrichtung **20** einwirken, um beispielsweise eine oder mehrere Zufallszahlen bzw. Ansteuersignale anzufordern.

[0027] Die Modussteuerungseinrichtung **22** greift auf die Kombinationseinrichtung **20** und die Ersetzungseinrichtung **12** über eine Modusleitung **26** zu, um abhängig von äußeren Situationen, wie z. B. bestimmten Programmteilen oder be-

stimmten erforderlichen Sicherheitsstufen von einer randomisierten Ersetzungsstrategie auf der Basis des physikalischen Zufallszahlengenerators **16** auf eine deterministische Ersetzungsstrategie entweder allein auf der Basis des Pseudozufallszahlengenerators oder unter Verwendung alternativer bekannter Ersetzungsstrategien umzuschalten.

[0028] Die Ersetzungseinrichtung **12** umfaßt LRU-Informationen **28a** für jede Datenspeichereinrichtung, um feststellen zu können, welche die am längsten nicht benutzte Datenspeichereinheit ist, um dann, wenn eine neue Datenmenge zu speichern ist, auf der Basis der LRU-Informationen **28a** die am längsten nicht benutzte Datenspeichereinheit durch die neue Datenspeichereinheit zu überschreiben. Die Ersetzungseinrichtung **12** hält bei einem bevorzugten Ausführungsbeispiel, das für die Umschaltung auf eine deterministische Speicherersetzung ausgebildet ist, die TAG-Informationen **28b** für jede Datenspeichereinheit, um einen assoziativen Datenspeicherzugriff zu schaffen. Mittels einer Adressenauswahlleitung **30** wird von der Ersetzungseinrichtung **12** auf die Datenspeichereinheiten zugegriffen, um eine Adressenauswahl für eine Ersetzung zu treffen. Ferner hat die Modussteuerungseinrichtung **22** eine weitere Ausgangsleitung **32**, um nicht nur die Ersetzungsmodusstrategie einzustellen, sondern auch eine Zeitintervallsteuerung für eine Umschaltung von einer Strategie in eine andere Strategie zu bewirken.

[0029] Die Kombinationseinrichtung **20** kann auf verschiedene Arten und Weisen physikalische Zufallszahlen von dem Zufallszahlengenerator **16** mit Pseudozufallszahlen von dem Pseudozufallszahlengenerator **18** kombinieren. Allgemein sind Pseudozufallszahlengeneratoren auf der Basis von rückgekoppelten Schieberegistern in der Lage, eine schnelle Sequenz von Pseudozufallszahlen zu erzeugen, während physikalische Zufallszahlengeneratoren im allgemeinen langsamer sind, so daß für bestimmte sehr schnelle Anwendungen der physikalische Zufallszahlengenerator, wenn er stromsparend sein soll und nur eine geringe Fläche in Anspruch nehmen darf, zu langsam ist. In so einem Fall kann die Kombinationseinrichtung **20** ausgebildet sein, um immer beispielsweise nach einer bestimmten Anzahl n von Pseudozufallszahlen eine physikalische Zufallszahl zur Adressauswahl direkt zu verwenden.

[0030] Bei einem alternativen Ausführungsbeispiel der vorliegenden Erfindung ist die Kombinationseinrichtung **20** ausgebildet, um immer Pseudozufallszahlen vom Pseudozufallszahlengenerator **18** zur Adressauswahl zu verwenden. Die physikalischen Zufallszahlen werden hierbei eingesetzt, um den Pseudozufallszahlengenerator neu zu "seeden". Dies bedeutet, daß der physikalische Zufallszahlengenerator immer dann, wenn eine neue physikalische Zufallszahl vorliegt, die Leitung **16b** aktiviert, um dann diese Zufallszahl der Kombinationseinrichtung **20** zuzuführen, die diese wiederum über die Leitung **18c** dem Zufallszahlengenerator **18** zuführt, so daß die rückgekoppelten Schieberegister in einen durch die Zufallszahl diktierten Anfangszustand versetzt werden. Durch ständiges Neu-Initialisieren des Pseudozufallszahlengenerators wird ein randomisiertes Stromprofil erreicht, das ferner bei einem Neustart des Systems nicht immer gleich ist, sondern lediglich für die ersten paar Cache-Ersetzungen bis zum ersten Neu-Initialisieren, wenn eine erste physikalische Zufallszahl vorliegt, gleich ist, dann jedoch zufällig und somit nicht durch die beschriebenen Angriffe erfaßbar ist.

[0031] Die Kombination eines Pseudozufallszahlengenerators mit einem physikalischen Zufallszahlengenerator hat daher die Vorteile, daß Zufallszahlen schnell genug erzeugt werden können, da physikalische Zufallszahlengeneratoren alleine im allgemeinen nicht genügend Zufallsbit mit genügend hoher Taktrate erzeugen können, wie sie in schnellen Prozessoren benötigt werden, und daß dennoch eine sichere Dekorrelation des Befehls- und/oder Datenstroms erreicht wird, da der Zufallszahlengenerator nicht vorhersagbare Zufallszahlen liefert, die zur Modifikation der Zufallsfolge des Pseudozufallszahlengenerators benutzt werden.

[0032] Darüber hinaus ist die Modussteuerungseinrichtung **22** ausgebildet, um während des Betriebs ("On the Fly") die Ersetzungseinrichtung **12** und die Kombinationseinrichtung **20** umzuschalten, und zwar zwischen einem oder mehreren deterministischen Ersetzungsstrategien und der nicht-deterministischen Strategie auf der Basis der physikalischen Zufallszahlen. Die deterministische Strategie kann beispielsweise LRU, Round-Robin, Pseudo-Random-Replacement oder eine andere bekannte Ersetzungsstrategie sein.

[0033] Die Umschaltung mittels der Modussteuerungseinrichtung **22** ist dahingehend vorteilhaft, daß in nicht-sicherheitsrelevanten Programmen oder Programmteilen, wo Leistungsangriffe unbedeutend sind, eine günstigere deterministische Ersetzungsstragegie gewählt werden kann. Eine deterministische Strategie ist auch dann wichtig, wenn garantierte und vorhersagbare Laufzeiten in zeit-kritischen Programmteilen nötig sind.

[0034] Bei einem weiteren Ausführungsbeispiel der Erfindung wird die Ersetzungseinrichtung über die Steuerleitung **32** angesteuert, um immer zwischen verschiedenen deterministischen Ersetzungsstrategien hin- und herzuschalten, und zwar abhängig von einer Zufallszahl des physikalischen Zufallszahlengenerators, die der Modussteuerungseinrichtung über eine Zufallszahlensteuerleitung **34** zugeführt wird. Es muß daher nicht immer eine Zufallsersetzungsstrategie auf der Basis von echten Zufallszahlen eingesetzt werden, sondern es kann auch zwischen verschiedenen deterministischen Ersetzungsstrategien hin- und hergeschaltet werden, wobei diese Hin- und Herschaltung auf der Basis echter physikalischer Zufallszahlen basiert, derart, daß ebenfalls eine Randomisierung des Verhaltens der Datenspeichervorrichtung erreicht wird, um Leistungsanalysen abzuwehren. Hierzu wird in regelmäßigen oder alternativen, nicht vorhersagbaren zeitlichen Intervallen, die von den physikalischen Zufallszahlen abhängen, die deterministische Strategie außer Kraft gesetzt und stattdessen eine zufällige Zeile für die Ersetzung ausgewählt, oder es wird eine deterministische Strategie durch eine andere deterministische Strategie ersetzt. Die Korrelation des Befehlsstroms wird also zum einen durch die zufällige Ersetzung, und zum anderen durch das zufällige Intervall gewährleistet. Immer werden die physikalischen Zufallszahlen des physikalischen Zufallszahlengenerators **16** verwendet, wodurch die Nicht-Vorhersagbarkeit des Verhaltens der Datenspeichervorrichtung sichergestellt wird.

[0035] Bei einem weiteren Ausführungsbeispiel der vorliegenden Erfindung ist die Modussteuerungseinrichtung **22** ferner ausgebildet, um das Umschaltintervall bzw. das Einstreu-Intervall, gemäß dem zufällig ausgewählte Zeilen ersetzt werden, einzustellen. Auf diese Weise kann dynamisch zur Laufzeit das Sicherheitsniveau eingestellt werden, indem die Intervallänge, mit der zufällig ausgewählte Zeilen "eingestreut" werden, größer oder kleiner gemacht werden.

[0036] Das erfindungsgemäße Konzept ist, wie es ausgeführt worden ist, dahingehend vorteilhaft, daß eine zeitliche Dekorrelation der Cache-Ersetzungsstrategie ohne die Verwendung von Leerfunktionsgeneratoren in einer CPU-Pipelinesteuerung erreicht wird. Das erfindungsgemäße Konzept zeichnet sich durch einen geringen Implementierungsaufwand und durch eine vernachlässigbare Leistungsverringerung aus. Insbesondere in einem assoziativen Cache-Spei-

cher mit dynamischer Umschaltung einer deterministischen Ersetzungsstrategie, wie z. B. Round-Robin, zu einer nichtdeterministischen Strategie unter Verwendung von physikalischen Zufallszahlen und gegebenenfalls zusätzlicher Verwendung von Pseudozufallszahlen wird eine sichere und effiziente Cache-Ersetzungsstrategie erreicht.

Bezugszeichenliste

10a Datenspeichereinheit
10b Adresse für die Datenspeichereinheit
12 Ersetzungseinrichtung
14 Leitung für neue Daten
16 Physikalischer Zufallszahlengenerator
16a Zufallszahlenleitung
16b RN-Valid-Leitung
16c Steuerleitung
18 Pseudozufallszahlengenerator
18a Pseudozufallszahlenleitung
18b PRN-Valid-Leitung
18c Steuerleitung
20 Kombinationseinrichtung
22 Modussteuerungseinrichtung
23 Leitung für Ansteuersignale
24 Steuerleitung
26 Ersetzungsstrategie-Auswahlleitung
28a LRU-Informationen
28b PEG-Informationen für einen assoziativen Zugriff
30 Adressauswahlleitung für eine Ersetzung
32 Intervallsteuerungsleitung
34 Zufallszahlen-Eingangsleitung

Patentansprüche

1. Datenspeichervorrichtung mit folgenden Merkmalen:
einer Mehrzahl von Datenspeichereinheiten (**10a**);
einem physikalischen Zufallszahlengenerator (**16**) mit einer Rauschquelle, die auf einem physikalischen Rauschprozeß basiert, zum Erzeugen einer Zufallszahl; und
einer Ersetzungseinrichtung (**12**) zum Auswählen einer Datenspeichereinheit, in der Daten zu speichern sind, abhängig von der Zufallszahl.

2. Datenspeichervorrichtung nach Anspruch 1, bei der die physikalische Rauschquelle des Zufallszahlengenerators (**16**) eine Schrotrauschquelle oder eine Quelle für thermisches Rauschen aufweist.

3. Datenspeichervorrichtung nach Anspruch 1 oder 2, die ferner folgendes Merkmal aufweist:
einen Pseudozufallszahlengenerator (**18**) zum Erzeugen einer Pseudozufallszahl;
eine Kombinationseinrichtung (**20**) zum Verwenden der Zufallszahl und der Pseudozufallszahl, um abhängig von der Zufallszahl und der Pseudozufallszahl ein Ansteuersignal (**22**) für die Ersetzungseinrichtung (**12**) zu liefern.

4. Datenspeichervorrichtung nach Anspruch 3, bei der die Kombinationseinrichtung (**20**) ausgebildet ist, um die Zufallszahl in den Pseudozufallszahlengenerator (**18**) als Keim einzuspeisen und eine von dem Pseudozufallszahlengenerator auf der Basis der Zufallszahl als Keim erzeugte Pseudozufallszahl als Ansteuersignal (**23**) für die Ersetzungseinrichtung zu verwenden.

5. Datenspeichervorrichtung nach Anspruch 3 oder 4, bei der die Ersetzungseinrichtung (**12**) ausgebildet ist, um eine Folge von Adressen auszuwählen, und bei der die Kombinationseinrichtung (**20**) ausgebildet ist, um Ansteuersignale für die Folge von Adressen so zu erzeugen, daß ein Ansteuersignal von der Zufallszahl abhängt und ein anderes Ansteuersignal von der Pseudozufallszahl abhängt.

6. Datenspeichervorrichtung nach einem der vorhergehenden Ansprüche, die ferner eine Modusteuerungseinrichtung (**22**) aufweist, die ausgebildet ist, um die Ersetzungseinrichtung so anzusteuern, daß in einem vorbestimmten Zeitintervall eine Ersetzung aufgrund einer Zufallszahl deaktiviert ist und stattdessen eine deterministische Ersetzungsstrategie eingesetzt wird.

7. Datenspeichervorrichtung nach Anspruch 6, bei der die Modussteuerungseinrichtung (**22**) ausgebildet ist, um eine deterministische Ersetzungsstrategie zu veranlassen, wenn nicht-sicherheitsrelevante Berechnungen in einem mit der Datenspeichervorrichtung gekoppelten Prozessor auszuführen sind, oder wenn für eine Berechnung durch den Prozessor garantierte oder vorhersagbare Laufzeiten gefordert sind.

8. Datenspeichervorrichtung nach Anspruch 6 oder 7, bei der die Modussteuerungseinrichtung (**22**) ausgebildet ist, um in regelmäßigen oder zufälligen Intervallen einen Wechsel der Ersetzungsstrategie zu veranlassen.

9. Datenspeichervorrichtung nach Anspruch 8, bei das zufällige zeitliche Intervall abhängig von einer Zufallszahl des physikalischen Zufallszahlengenerators durch die Modussteuerungseinrichtung (**22**) bestimmbar ist.

10. Datenspeichervorrichtung nach Anspruch 1, die ferner eine Modussteuerungseinrichtung (**22**) aufweist, die ausgebildet ist, um eine Zufallszahl des physikalischen Zufallszahlengenerator über eine Zufallszahlleitung (**34**) zu erhalten, und die ferner ausgebildet ist, um abhängig von der Zufallszahl eine einer Mehrzahl von verschiedenen deterministischen Ersetzungsstrategien für die Ersetzungseinrichtung (**12**) auszuwählen.

11. Datenspeichervorrichtung nach einem der vorhergehenden Ansprüche, die als assoziativer Cache-Speicher ausgeführt ist.

12. Verfahren zum Ersetzen eines Inhalts einer Datenspeichervorrichtung, die eine Mehrzahl von Datenspeichereinheiten aufweist, mit folgenden Schritten:
Liefern einer von einem physikalischen Rauschprozeß abhängigen Zufallszahl;
Auswählen einer Datenspeichereinheit der Mehrzahl von Datenspeichereinheiten abhängig von der physikalischen Zufallszahl; und
Speichern von zu speichernden Daten in der ausgewählten Datenspeichereinheit.

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 102 16 611 A1
Int. Cl.[7]: G 06 F 12/08
Offenlegungstag: 6. November 2003

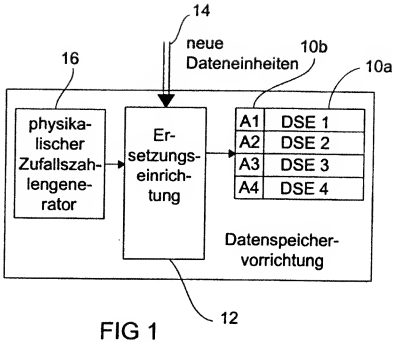


FIG 1

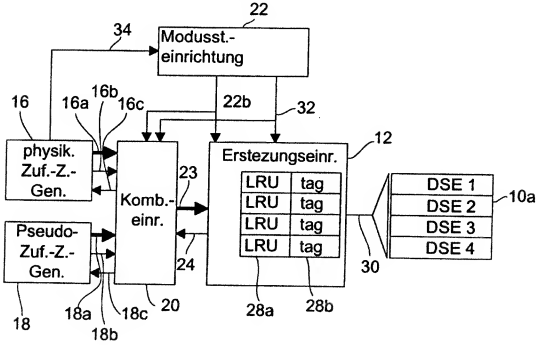


FIG 2